Annual 47 CFR § 64.2009(e) CPNI Certification Template
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: February 27, 2018
2. Name of company(s) covered by this certification: Development Authority of the North Country
3. Form 499 Filer ID: 823896
4. Name of signatory: James W. Wright
5. Title of signatory: executive Director
6. Certification:

I, James W. Wright, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 CFR § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 CFR § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____

Attachments: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers – (if applicable) – N/A
Summary of customer complaints (if applicable) – N/A

Annual 47 C.F.R. §64.2009(e) CPNI Certification for 2018

EB Docket No. 06-36

STATEMENT OF PROCEDURES

Development Authority of the North Country, Form 499 Filer 823896 ("Company") offers intrastate private line and transport services on a wholesale basis to other carriers and offers dark fiber optic services within the State of New York. As a carrier's carrier, the Company neither receives nor obtains consumer proprietary network information ("CPNI"). In the event the Company in the future receives or obtains CPNI, the Company has established operating procedures that ensure compliance with the Federal Communications Commission ("Commission") regulations regarding the protection of CPNI.

- Company maintains a CPNI Policy to ensure that its customer's CPNI adequately will be protected from unauthorized disclosure and that the Company operating procedures comply with the Commission's CPNI rules.

- Company educates and trains its employees annually regarding the appropriate use of CPNI. New employees who will have access to CPNI initially are educated and trained upon commencement of their employment. Company has established disciplinary procedures should an employee violate the CPNI procedures established by Company.

- Company understands that it may use, disclose or permit access to CPNI in only three circumstances: (1) as required by law; (2) with the customer's approval; and (3) in providing the service from which the CPNI is derived.

    - Company may use, disclose or permit access to CPNI, without customer approval (i) to market enhancements to services already used by the customer; (ii) to initiate, render, bill and collect for telecommunications services; (iii) to protect the Company's rights or property or to protect users of those services and other carriers from fraudulent, abusive or unlawful use of, or subscription to, such services; and (iv) as may be required by law.

    - Company does not use, disclose or permit access to CPNI to market to a customer service offerings that are within a category of service to which the customer does not already subscribe from Company, unless Company has customer approval to do so.

    - Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

    - Company will disclose CPNI to any person designated by the customer only upon the affirmative written request by the customer

- When customer consent is required to use, disclose or permit access to customer's CPNI, Company will obtain customer consent through written, oral or electronic methods. Company honors customer's approval or disapproval to use, disclose or permit access to CPNI until the customer revokes or limits such approval.

- In the event that the Company in the future receives or obtains CPNI, Company will implement a system to password protect online access to CPNI.

- Prior to any solicitation for customer approval, Company individually will notify and inform its customers of their right to restrict the use or disclosure of and access to CPNI. Company may use the "opt-out" method or the "opt-in" method to obtain customer approval to use or share CPNI.

- In the event Company in the future receives or obtains CPNI and uses CPNI to market to its customers, Company has implemented a system whereby it will maintain a record of its sales and marketing campaigns that may use its customers' CPNI. Company also has implemented a system whereby it will maintain a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record will include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. These records will be maintained in either electronic or paper form for a minimum of one year.

- Company does not have any corporate affiliates and does not share CPNI with any third parties for marketing purposes. Company has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations. Specifically, Company's sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI. Company maintains records in either electronic or paper form of Company compliance for a minimum period of one year.

- Company has implemented a notification process for both law enforcement and customers in the event of a CPNI breach. Prior to notifying its customers, as soon as practicable, and in no event later than seven business days, after reasonable determination of the breach, Company shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central report facility. Notwithstanding any state law to the contrary, Company shall not notify customers or disclose the breach to the public until seven full business days have passed after notification to the USSS and the FBI except: (A) If Company believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. Company shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification, or (B) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal

investigation or national security, such agency may direct Company not to so disclose or notify for an initial period of up to thirty days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency.

- Company shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI, and notifications made to customers. The record shall include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Company shall retain the record for a minimum of two years.